servicenow

What is your Exposure to Ransomware?

Assess yourself to uncover ways to reduce your attack surface and response time.

When it rains, it pours. Ransom demands are up, and the cost of clean-up has doubled in the last year.

Combating ransomware requires a mix of proactive hygiene, risk-based preparation, and rapid and surgical response. Most things you should do help against any attack, and some help with risk and compliance concerns.

What's causing the current spike?

1) Focus on vulnerable targets: Because they have a short window of acceptable downtime, critical infrastructure and supply chains are being increasingly victimized.
2) Strikes can come from anywhere. Crime gangs can tap the expanding international cloud infrastructure to easily attack organizations across the planet—with little fear of extradition.
3) Ransomware-as-a-service (RaaS): Powerful encryption tools, communications routes, and ransom collection methods can be bought from nefarious franchisers to help criminals do their deeds.

Ransomware is now also being used in data extortion attacks, where data is stolen with the threat of public disclosure to damage organizational, employee, or customer reputation and compliance.

Take this quiz to uncover ways ServiceNow can help reduce your exposure to attack.

What matters to your organization?

Attackers figure out what disabled services or leaked data could most cripple your operations or reputation, and target that. Supply chains amplify the impact. A risk-based approach helps you prioritize all your actions.

- What are the most important business- or mission-critical services supporting your customers, employees, or the products and services that enable your purpose?
- What is the impact of an hour or a day of downtime for these services?
- What regulations and compliance obligations would be affected by a ransomware attack?
- Which vendors and suppliers are most critical to your operations?

70% of all system intrusion breaches involved malware, with ransomware making up 99% of those cases.[1]

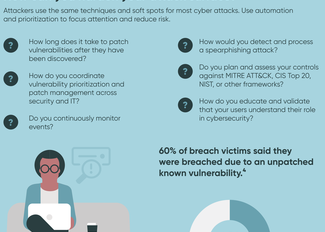
Sensitive data is stolen before being encrypted, so victims can be threatened with exposure if the ransom isn't paid. Data on employees and customers allows extortion from users as well as the targeted organization.

ServiceNow can help you orchestrate recovery efforts across your organization to respond to disruptions 40% faster.[2]
Consider Business Continuity Management, Integrated Risk Management, Vulnerability Response, Inspire Value Assessment.

What is your attack surface?

Internet-facing systems, unsupported and forgotten devices, and systems with privileged access to other systems are favorite targets. Don't forget to look at access and cybersecurity practices by your suppliers and third-party providers.

- Do you know where your regulated and sensitive data is stored?
- How do you assess the risk to your supply chain?
- Can you map out the components of your critical services?
- Do you have any specialized systems related to your business or industry?
- How do you identify and decommission unused and EOL devices and software?
- How confident are you in the accuracy of this hardware and software inventory?
- Do you know who "owns" maintaining them?



Forrester identified a 70% improvement in the way organizations identify and prioritize vulnerabilities and assess the impact on existing assets.[3]
Consider ServiceNow Discovery, Connected Operations, Service Mapping, Asset Management, CMDB, Vendor Risk Management, Vulnerability Response.

How can you harden your attack surface?

Attackers use the same techniques and soft spots for most cyber attacks. Use automation and prioritization to focus attention and reduce risk.

- How long does it take to patch vulnerabilities after they have been discovered?
- How do you coordinate vulnerability prioritization and patch management across security and IT?
- Do you continuously monitor events?
- How would you detect and process a spearphishing attack?
- Do you plan and assess your controls against MITRE ATT&CK, CIS Top 20, NIST, or other frameworks?
- How do you educate and validate that your users understand their role in cybersecurity?

60% of breach victims said they were breached due to an unpatched known vulnerability.[4]

With ServiceNow, organizations have automated phishing and malware playbooks driving a 30% improvement in vulnerability response times.[3]
Consider ServiceNow Vulnerability Response, Threat Intelligence, Security Incident Response, CMDB, Asset Management, ITSM, Integrated Risk Management, Employee Workflows.

How can you optimize your ransomware response?

By planning ahead, formalizing and automating as much as possible, and practicing, you can be prepared to move quickly to detect, contain, and reduce any sort of external attack or insider threat activity.

- Does your team have formal playbooks for security incident response?
- How many people would be involved in response, and from which groups?
- How would you organize and communicate during the process?
- Are executive, regulatory, and public communications included in your response plan?
- How recently have you practiced a major security incident response?
- What tools does your CISO have to understand performance?

In 2021, 39% of ransomware attacks were stopped before the data could be encrypted.[5]

For security incidents requiring coordination across IT and security, ServiceNow customers average a 40% improvement in handling tier 1 and a 60% efficiency in tier 2 and higher.[3]
Consider ServiceNow Security Incident Response, Business Continuity Management, Performance Analytics

ServiceNow workflows for security operations, IT, and risk management run on a single architecture with a common data model. With our partner ecosystem and playbooks, we help customers shore up ransomware readiness in key areas. **Let's partner to build an action plan addressing the big picture of your cybersecurity.**

Resources

Reduce Your Exposure to Targeted Ransomware and Ransomware as a Service (RaaS)

The Destructive Rise of Ransomware as a Service

Threat Hunting with Security Incident Response, and Vulnerability Response with ServiceNow for SUNBURST and SUPERNOVA Attacks

Security Operations Use Case Guide

All Together Now: How security and IT teams can work together to drive operational resilience

Shrink Your Attack Surface

Quickly Put Out Fires with an Exposure Assessment

www.servicenow.com/security/operations

Sources

[1] https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

[2] https://www.servicenow.com/lpay/forrester-the-total-economic-impact-of-servicenow-governance-risk-and-compliance.html

[3] https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

[4] https://www.servicenow.com/lpay/ponemon-vulnerability-survey.html

[5] https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

[6] https://www.servicenow.com/lpay/forrester-the-total-economic-impact-of-servicenow-security-operations.html

servicenow

servicenow.com